IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

IN RE: BLACKBAUD, INC., CUSTOMER DATA BREACH LITIGATION	Case No.: 3:20-mn-02972-JMC MDL No. 2972 **ORDER AND OPINION**

THIS DOCUMENT RELATES TO: ALL ACTIONS:

This matter is before the court on Defendant Blackbaud, Inc.'s ("Blackbaud") Motion to Dismiss seven (7) of Plaintiffs' statutory claims pursuant to Federal Rule of Civil Procedure 12(b)(6). (ECF No. 110.) For the reasons set forth below, the court **GRANTS IN PART** and **DENIES IN PART** Blackbaud's Motion. (*Id.*)

I. RELEVANT BACKGROUND

Blackbaud is a publicly traded cloud software company incorporated in Delaware and headquartered in Charleston, South Carolina. (ECF No. 77 at 110-11 ¶ 419, 112 ¶ 424.) The company provides data collection and maintenance software solutions for administration, fundraising, marketing, and analytics to social good entities such as non-profit organizations, foundations, educational institutions, faith communities, and healthcare organizations ("Social Good Entities"). (*Id.* at 4 ¶ 4, 114 ¶ 430.) Blackbaud's services include collecting and storing Personally Identifiable Information ("PII") and Protected Health Information ("PHI") from its customers' donors, patients, students, and congregants. (*Id.* at 3 ¶ 2, 114 ¶ 429.)

In this action, Plaintiffs represent a putative class of individuals whose data was provided to Blackbaud's customers and managed by Blackbaud. (*Id.* at 6 ¶ 12.) Thus, Plaintiffs are patrons

of Blackbaud's customers rather than direct customers of Blackbaud. (ECF Nos. 92-1 at 9; 109 at 7-8.)

Plaintiffs assert that from February 7, 2020 to May 20, 2020, cybercriminals orchestrated a two-part ransomware attack on Blackbaud's systems ("Ransomware Attack"). (ECF No. 77 at 11-12 ¶ 25.) Cybercriminals first infiltrated Blackbaud's computer networks, copied Plaintiffs' data, and held it for ransom. (*Id.* at 11 ¶ 25, 137 ¶ 496; ECF No. 92-1 at 7.) When the Ransomware Attack was discovered in May 2020, the cybercriminals then attempted but failed to block Blackbaud from accessing its own systems. (*Id.*) Blackbaud ultimately paid the ransom in an undisclosed amount of Bitcoin in exchange for a commitment that any data previously accessed by the cybercriminals was permanently destroyed. (ECF Nos. 77 at 9 ¶ 20, 138 ¶ 499; 92-1 at 7.)

Plaintiffs maintain that the Ransomware Attack resulted from Blackbaud's "deficient security program[.]" (ECF No. 77 at 117-18 ¶ 439.) They assert that Blackbaud failed to comply with industry and regulatory standards by neglecting to implement security measures to mitigate the risk of unauthorized access, utilizing outdated servers, storing obsolete data, and maintaining unencrypted data fields. (*Id.* at 117-18 ¶ 439, 134 ¶ 486, 136 ¶ 491, 142 ¶ 510.)

Plaintiffs further allege that after the Ransomware Attack, Blackbaud launched a narrow internal investigation into the attack that analyzed a limited number of Blackbaud systems and did not address the full scope of the attack. (*Id.* at 143 ¶ 514.) On July 14, 2020, Blackbaud received the investigation report ("Forensic Report") which acknowledged that "names, addresses, phone numbers, email addresses, dates of birth, and/or SSNs" were disclosed in the breach but stated that the investigation was "unable to detect credit card data while reviewing exfiltrated data[.]" (*Id.* at 143 ¶ 514 n.112, 144 ¶ 516, 154 ¶ 549.) Plaintiffs claim the Forensic Report "improperly

concludes that no credit card data was exfiltrated" because "such data could have existed in the unexamined database files." (*Id.* at 144 ¶ 516.)

Plaintiffs contend that Blackbaud failed to provide them with timely and adequate notice of the Ransomware Attack and the extent of the resulting data breach. (*Id.* at 130-31 ¶ 473.) They claim that they did not receive notice of the Ransomware Attack "until July of 2020 at the earliest[.]" (*Id.* at 156 ¶ 555.) On July 16, 2020, The NonProfit Times reported that Blackbaud had been the subject of a ransomware attack and data breach and Blackbaud issued a statement about the Ransomware Attack on its website. (*Id.* at 9 ¶ 20, 138 ¶ 499.) In both disclosures, Blackbaud asserted that the cybercriminals did not access credit card information, bank account information, or SSNs. (*Id.*)

Plaintiffs allege that they subsequently received notices of the Ransomware Attack from various Blackbaud customers at different points in time from July 2020 to January 2021. (*See, e.g.*, *id.* at 25 ¶ 63, 29 ¶ 82, 32 ¶ 93, 109 ¶ 414.) They maintain that some of the notices stated that SSNs, credit card data, and bank account information were not accessed during the Ransomware Attack while others stated that SSNs but not credit card data or bank account information were exposed during the Ransomware Attack. (*See, e.g.*, *id.* at 25 ¶ 64, 29 ¶ 82, 52 ¶ 173, 65 ¶ 230.)

Plaintiffs maintain that although Blackbaud initially represented that sensitive information such as SSNs and bank account numbers were not compromised in the Ransomware Attack, Blackbaud informed certain customers in September and October 2020 that SSNs and other sensitive data were in fact stolen in the breach. (*Id.* at 141-42 ¶ 509.) Additionally, on September 29, 2020, Blackbaud filed a Form 8-K with the Securities and Exchange Commission stating that SSNs, bank account information, usernames, and passwords may have been exfiltrated during the Ransomware Attack. (*Id.* at 12 ¶ 26, 143 ¶ 512.)

After the Ransomware Attack was made public, putative class actions arising out of the intrusion into Blackbaud's systems and subsequent data breach were filed in state and federal courts across the country. (ECF No. 1 at 1.) On December 15, 2020, the Judicial Panel on Multidistrict Litigation consolidated all federal litigation related to the Ransomware Attack into this multidistrict litigation ("MDL") for coordinated pretrial proceedings.[1] (*Id.* at 3.)

On April 2, 2021, thirty-four (34) named Plaintiffs[2] from twenty (20) states filed a Consolidated Class Action Complaint ("CCAC") alleging that their PII and/or PHI was compromised during the Ransomware Attack. (ECF No. 77.)[3] They assert six (6) claims on behalf of a putative nationwide class as well as ninety-one (91) statutory claims on behalf of putative state subclasses. (*Id.* at 173 ¶ 627 – 424 ¶ 1815.)

To facilitate the efficient resolution of the litigation, the court ordered that the first phase of motions practice address jurisdictional issues, certain statutory claims, and specific common law claims. (ECF Nos. 23 at 2; 78 at 1.) On May 3, 2021, Blackbaud filed a Motion to Dismiss for Lack of Subject Matter Jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) ("Jurisdictional Motion to Dismiss"). (ECF No. 92.) The court denied Blackbaud's Jurisdictional Motion to Dismiss on July 1, 2021. (ECF No. 121.)

Blackbaud filed the instant Motion to Dismiss pursuant to Rule 12(b)(6) on June 4, 2021, contending that Plaintiffs' California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code

[1] As of August 12, 2021, this MDL is comprised of twenty-nine (29) member cases.

[2] All named Plaintiffs are identified in paragraphs forty-five (45) through 418 of the CCAC. (*See* ECF No. 77 at 20 ¶ 45 – 110 ¶ 418.)

[3] The CCAC supersedes all other complaints in this MDL filed on behalf of Blackbaud's customer's patrons against Blackbaud. (ECF Nos. 23 at 4; 77.) Although the docket reflects that the CCAC was not publicly filed until April 16, 2021, Plaintiffs provided Blackbaud and the court with the CCAC on April 2, 2021 to facilitate the sealing process and maintain the cadence of this litigation. (ECF Nos. 66; 72; 76; 77.)

§§ 1798.100–1798.199.95; California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §§ 56–56.265; Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201–501.213; New Jersey Consumer Fraud Act ("NJCFA"), N.J. Stat. Ann. §§ 56:8-1–56:8-20; New York General Business Law ("GBL") § 349; Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 P.S. §§ 201-1–201-9.2; and South Carolina Data Breach Security Act ("SCDBA"), S.C. Code Ann. § 39-1-90, claims (collectively, "Select Statutory Claims") should be dismissed for failure to state a claim. (ECF No. 110.) Plaintiffs filed a Response on July 6, 2021. (ECF No. 123.) The court held a hearing on the Motion on July 20, 2021. (ECF Nos. 136, 137.)

II. LEGAL STANDARD

A. Applicable Law

In federal diversity actions, federal law governs procedural issues and state law governs substantive issues. *See Dixon v. Edwards*, 290 F.3d 699, 710 (4th Cir. 2002). In the MDL context, a transferee court must apply federal law as interpreted by the circuit where the transferee court sits to matters of procedure. *See, e.g.*, *In re Porsche Cars North America, Inc.*, 880 F. Supp. 2d 801, 815 (S.D. Ohio 2012); *McGuffie v. Mead Corp.*, 733 F. Supp. 2d 592, 594 (E.D. Pa. 2010). Accordingly, the court will apply the United States Court of Appeals for the Fourth Circuit's interpretation of federal procedural law. In contrast, the court "must apply the jurisprudence of the relevant state's highest court or, if it has not spoken to the issue, predict how the state's highest court would rule" to analyze Plaintiffs' state statutory claims. *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 467 (D. Md. 2020) (citing *Erie Railroad Co. v. Tompkins*, 304 U.S. 64, 58 (1938); *Private Mortg. Inv. Servs., Inc. v. Hotel & Club Assocs., Inc.*, 296 F.3d 308, 312 (4th Cir. 2002)).

B. Motion to Dismiss

A motion to dismiss pursuant to Rule 12(b)(6) "challenges the legal sufficiency of a complaint." *Francis v. Giacomelli*, 588 F.3d 186, 192 (4th Cir. 2009). It is not intended to "'resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses.'" *Presley v. City of Charlottesville*, 464 F.3d 480, 483 (4th Cir. 2006) (quoting *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999)).

A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Thus, "[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Twombly*, 550 U.S. at 556). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (citing *Twombly*, 550 U.S. at 556).

When considering a Rule 12(b)(6) motion to dismiss, the court must accept all well-pled factual allegations as true and view the complaint in the light most favorable to the plaintiff. *See e.g.*, *Aziz v. Alcolac*, 658 F.3d 388, 391 (4th Cir. 2011); *Ostrzenski v. Seigel*, 177 F.3d 245, 251 (4th Cir. 1999). However, the court is not required to accept legal conclusions as true. *Aziz*, 658 F.3d at 391 (citing *Iqbal*, 556 U.S. at 680).

To survive a motion to dismiss, "claims of fraud" must satisfy both Rule 8(a)'s plausibility requirement and Federal Rule of Civil Procedure 9(b)'s particularity standard. *Xia Bi v. McAuliffe*, 927 F.3d 177, 182 (4th Cir. 2019). Rule 9(b) imposes a heightened pleading standard on fraud

claims, requiring a plaintiff to "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). The Rule 9(b) particularity standard requires a party to, "at a minimum, describe 'the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby.' These facts are often 'referred to as the who, what, when, where, and how of the alleged fraud.'" *Bakery & Confectionary Union & Indus. Int'l Pension Fund v. Just Born II, Inc.*, 888 F.3d 696, 705 (4th Cir. 2018) (quoting *U.S. ex rel. Wilson v. Kellogg Brown & Root, Inc.*, 525 F.3d 370, 379 (4th Cir. 2008)). Rule 9(b)'s heightened pleading requirements apply to state law claims litigated in federal court. *Topshelf Mgmt., Inc. v. Campbell-Ewald Co.*, 117 F. Supp. 3d 722, 726 (M.D.N.C. 2015) (citing *U.S. ex rel. Palmieri v. Alpharma, Inc.*, 928 F. Supp. 2d 840, 853 (D. Md. 2013)).

As the court will decide the instant Motion to Dismiss before class certification, the court's rulings will only bind the named Plaintiffs. MANUAL FOR COMPLEX LITIGATION (FOURTH) § 21.11 (2004) ("Motions such as challenges to jurisdiction and venue, motions to dismiss for failure to state a claim, and motions for summary judgment may be decided before a motion to certify the class, although such precertification rulings bind only the named parties.").

III. ANALYSIS

Blackbaud contends that the court should dismiss Plaintiffs' Select Statutory Claims for failure to state a claim. (ECF No. 110 at 10.) The court will address each claim in turn.

A. California Consumer Privacy Act Claims

California Plaintiffs Kassandre Clayton ("Clayton"), Philip Eisen ("Eisen"), Mamie Estes ("Estes"), and Shawn Regan ("Regan") (collectively, "California Plaintiffs") allege claims under the CCPA. (ECF No. 77 at 214 ¶ 819 – 216 ¶ 833.) The CCPA

> provides a private right of action for actual or statutory damages to "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an

> unauthorized access and exfiltration, theft, or disclosure as a result of the ***business's*** violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information[.]"

Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020) (quoting Cal. Civ. Code § 1798.150(a) (West 2021)) (emphasis added). Blackbaud contends California Plaintiffs' CCPA claims fail as a matter of law because Blackbaud is not a "business" regulated by the Act. (ECF No. 110-1 at 19.)

Since the CCPA only applies to data breaches that occurred after January 1, 2020, courts have had few opportunities to dissect the Act's provisions. *See Gardiner v. Walmart Inc.*, No. 20-CV-04618-JSW, 2021 WL 2520103, at *2 (N.D. Cal. Mar. 5, 2021) (finding that data breaches are only actionable under the CCPA if they occur after January 1, 2020). However, the plain text of the statute is instructive.

The CCPA defines a "business" as a for-profit entity (1) "that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information[;] or" (2) "on the behalf of which that information is collected[;] or" (3) "that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information[.]" Cal. Civ. Code § 1798.140(c) (West 2021). Such an entity must also meet one (1) of the following thresholds to qualify as a "business" under the CCPA: (A) have annual gross revenues in excess of $25 million; (B) annually buy, receive, sell, or share the personal information of 50,000 or more consumers, households, or devices; or (C) earn more than half of its revenue from selling consumers' personal information. *Id.*

Here, California Plaintiffs adequately allege that Blackbaud qualifies as a "business" under the CCPA. First, they specifically maintain that "Blackbaud and its direct customers determine the purposes and means of processing consumers' personal information. Blackbaud uses

consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test Blackbaud's services." (ECF No. 77 at 215 ¶ 823.) The CCAC is also filled with claims that Blackbaud develops software solutions to process its customers' patrons' personal information. (*See, e.g.*, *id.* at 7 ¶ 15 ("Blackbaud markets itself to Social Good Entities by developing data-hosting 'solutions' to meet those entities' needs"); 115 ¶ 433 ("Blackbaud determines the purposes or means of processing customers' data based on which solutions or services are utilized by the customers"); 116 ¶ 436 (Blackbaud offers "professional and managed services in which its expert consultants provide data conversion, implementation, and customization services for each of its software solutions").) Second, the California Plaintiffs contend that Blackbaud has "annual gross revenues over $25 million." (*Id.* at 214 ¶ 821.)

Blackbaud's status as a "business" under the CCPA is further supported by Blackbaud's alleged registration as a "data broker" in California. California Plaintiffs claim that Blackbaud is registered as a "data broker" in California pursuant to Cal. Civ. Code § 1798.99.80. (*Id.* at 215 ¶ 824.) Cal. Civ. Code § 1798.99.80 provides that a "data broker" is a "***business*** that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80(d) (West 2021) (emphasis added). The provision also explicitly employs the same definition of "business" as the CCPA, Cal. Civ. Code § 1798.140(c). Cal. Civ. Code § 1798.99.80(a) (West 2021) ("(a) 'Business' has the meaning provided in subdivision (c) of Section 1798.140."). Since an entity must qualify as a "business" under the CCPA in order to be registered as a "data broker" in California, Blackbaud's alleged registration as a "data broker" suggests that it is also a "business" under the CCPA.

Finally, the court rejects Blackbaud's argument that Blackbaud is not a "business" under the CCPA because it qualifies as a "service provider" under the Act. (ECF No. 110-1 at 19.) The CCPA defines "service provider" as

> a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

Cal. Civ. Code § 1798.140(v) (West 2021). In other words, a "service provider" is a for-profit organization that processes consumer personal information on behalf of a business pursuant to a contract. Thus, a "service provider" could also qualify as a "business" because a "business" is a for-profit organization "that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information[.]" Cal. Civ. Code § 1798.140(c) (West 2021). Accordingly, the statutory definition of "service provider" suggests that "business" is a broader term that encompasses "service provider." Such an interpretation is consistent with the CCPA's direction that the Act "be liberally construed to effectuate its purposes" to "further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information[.]" Cal. Civ. Code §§ 1798.175, 1798.194 (West 2021).

Because Blackbaud could be both a "service provider" and a "business" under the CCPA, it would not be insulated from liability under the CCPA if it qualified as a "service provider." Consequently, the court need not consider whether Blackbaud is a "service provider" under the CCPA to resolve the Motion to Dismiss presently before the court. (ECF No. 110.)

As California Plaintiffs adequately assert that Blackbaud constitutes a "business" under the CCPA, they sufficiently allege violations of the CCPA. Accordingly, the court denies Blackbaud's Motion to Dismiss California Plaintiffs' claims under the CCPA. (*Id.*)

B. California Confidentiality of Medical Information Act Claims

California Plaintiffs also assert claims under California's CMIA. (ECF No. 77 at 214 ¶ 819 – 216 ¶ 833.) The CMIA prohibits a "provider of health care" from disclosing a patient's "medical information" without authorization except in certain specified instances. Cal. Civ. Code § 56.10(a) (West 2021). Blackbaud asserts that California Plaintiffs' CMIA claims should be dismissed because their "medical information" was not exposed as a result of the Ransomware Attack and Blackbaud does not qualify as a "provider of health care" under the CMIA. (ECF No. 110-1 at 23-27.)

California's CMIA applies to "[a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information." Cal. Civ. Code § 56.06(b); *see also* Valerie J. Lopez, *Health Data Privacy: How States Can Fill the Gaps in HIPAA*, 50 U.S.F.L. 313, 326 (2016) (stating "California's CMIA applies to any business that maintains or offers software that maintains medical information.") (citing Cal. Civ. Code § 56.06(b) (West 2013)). The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(j) (West 2021). Thus, "a prohibited release by a health care provider must include more than individually identifiable information but must also include information relating to medical history, mental or physical condition, or treatment of the individual" to constitute "medical

information." *Eisenhower Med. Ctr. v. Superior Court*, 172 Cal. Rptr. 3d 165, 170 (Cal. Ct. App. 2014).

Here, Eisen, Estes, and Regan have not plausibly alleged that "information relating to [their] medical history, mental or physical condition, or treatment" was disclosed during the Ransomware Attack, thus they have failed to sufficiently assert that their "medical information" was exposed as a result of the data breach. *Eisenhower*, 172 Cal. Rptr. 3d at 170. Estes and Regan claim that their names, SSNs, and tax identification numbers were exposed while Eisen maintains that his street addresses and telephone numbers were compromised. (ECF No. 77 at 25 ¶ 63, 27 ¶ 72, 29 ¶ 82.) All assert that it is unknown how much of their PII was exposed during the Ransomware Attack, but none maintain that their PHI could have been compromised. (*Id.* at 25 ¶ 64, 27 ¶ 74, 30 ¶ 84.) It is also not plausible that Eisen's, Estes', and Regan's "medical information" was disclosed during the Ransomware Attack because they allege that their PII was exposed as a result of their relationships with non-profit organizations rather than their interactions with medical providers. Thus, they do not state claims under the CMIA.

However, Clayton plausibly alleges that her "medical information" was disclosed during the Ransomware Attack. She claims Community Medical Centers notified her that her name, address, phone number, email address, date of birth, room number, patient identification number, name of hospital where treated, and applicable hospital department or unit may have been exposed and Trinity Health informed her that her name, address, phone number, email, most recent donation date, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number and physician name were exposed. (ECF No. 77 at 22 ¶ 52.) Furthermore, Clayton contends that "additional medical information, such as [her] diagnosis or treatment plan" may have also been compromised due to Blackbaud's lack of transparency about the scope of the

Ransomware Attack. (*Id.* at 22 ¶ 53.) Therefore, the information Clayton alleges was compromised in the Ransomware Attack shows when and where she received medical treatment, which doctors treated her, and whether her treatment required an inpatient stay. If more information was exposed during the Ransomware Attack than initially reported, it may also reveal her medical history, mental and/or physical condition, and specific treatments. Accordingly, Clayton has plausibly alleged that "information relating to [her] medical history, mental or physical condition, or treatment" was exposed during the Ransomware Attack. *Eisenhower*, 172 Cal. Rptr. 3d at 170.

The CMIA's definition of "provider of health care" encompasses traditional medical providers such as nurses, doctors, and hospitals. Cal. Civ. Code § 56.05(m) (West 2021). But in order "to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider[,]" the CMIA's definition of "provider of health care" also includes entities that are not ordinarily considered medical providers, such as technology companies that process and maintain "medical information." *Brown v. Mortensen*, 253 P.3d 522, 533 (Cal. 2011) (explaining the protective purpose of the CMIA); Cal. Civ. Code § 56.06(b) (West 2021) ("Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information . . . shall be deemed a provider of healthcare subject to the requirements of this part."). Notably, the CMIA was amended in 2013 to clarify its application to businesses that maintain or offer software that maintains medical information. *See* A.B. 658, chap. 296, 2013 Leg. (Cal. 2013), amending Cal. Civ. § 56.06(b); *see also* Assembly Committee on Appropriations, Bill Analysis, A.B. 658 (May 1, 2013). Specifically, the CMIA defines "provider of health care" in relevant part as

> [a]ny business that offers software or hardware to consumers . . . in order to make the information available to an individual or a provider of health care at the request

> of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual . . . .

Cal. Civ. Code § 56.06(b) (West 2021). The purpose of the 2013 amendment of CMIA § 56.06 was to close a loophole "by applying the existing statutory provisions to the newest platform for commercial vendors who offer storage, maintenance, and sharing of sensitive medical information." Lopez, *Health Data Privacy*, *supra*, at 327 (citing Assembly Committee on Appropriations, Bill Analysis, A.B. 658 (May 1, 2013)). Blackbaud falls within this category.

Blackbaud first maintains that it is not a "provider of health care" under Cal. Civ. Code § 56.06(b) because "California Plaintiffs never had direct contact with Blackbaud and at no point purchased a product from Blackbaud." (ECF No. 110-1 at 25.)[4] This argument fails. The statute does not require a business to offer software or hardware directly to a plaintiff in order to qualify as a "provider of health care." In fact, the text of the statute provides that a technology company can be a "provider of health care" even if the "individual" whose information is managed by the technology and the "provider of health care" using the technology are not "consumers" of the technology. *See* Cal. Civ. Code § 56.06(b) (West 2021). Moreover, the statutory language suggests that the definition of "consumers" is not limited to "individuals" because it uses both terms. *See id.* ("[a]ny business that offers software or hardware to ***consumers*** . . . in order to make the information available to an ***individual***") (emphasis added).

Second, Blackbaud argues that it cannot be a "provider of health care" because California Plaintiffs fail to allege that Blackbaud collected their information "for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a

[4] As there is presently no case law interpreting Cal. Civ. Code § 56.06(b), the court will rely on the text of the statute and legislative history to resolve Blackbaud's challenge.

medical condition of the individual[.]" (ECF No. 110-1 at 26 (citing Cal. Civ. Code § 56.06(b) (West 2021)).) In amending Cal. Civ. Code § 56.06 to include businesses that maintain or offer software that maintains medical information, the California legislature intended to ensure that the CMIA would apply to all businesses that maintain medical information "whether or not the business was organized for that purpose." Joseph R. Tiffany et al., *The Doctor is in, but your Medical Information is Out*, 24 No. 1 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 206, 225 (2015); *see also* Assembly Committee on Appropriations, Bill Analysis, A.B. 658 (May 1, 2013).

The court observes that Blackbaud's argument requires a tortured reading of the CMIA. Cal. Civ. Code § 56.06(b) does not suggest that a business can only be a "provider of health care" if its software or hardware is used "for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual[.]" Cal. Civ. Code § 56.06(b) (West 2021). Instead, a business can qualify as a "provider of health care" if it offers software or hardware to consumers (1) "in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care," (2) "for purposes of allowing the individual to manage his or her information, or" (3) "for the diagnosis, treatment, or management of a medical condition of the individual[.]" *Id.*

California Plaintiffs plausibly allege that Blackbaud offered its software for such uses. They specifically claim that "Blackbaud's systems were designed, in part, to make medical information available to Social Good Entities by providing cloud-based computing solutions through which those organizations could store, access, and manage consumers' medical information, including but not limited to diagnosing, treating, or managing consumers' medical

conditions." (ECF No. 77 at 217 ¶ 840.) Clayton also maintains that she was "required to provide her PHI to several healthcare providers as a predicate to receiving healthcare services" and her "PHI was in turn provided to Blackbaud to be held for safekeeping." (*Id.* at 22 ¶ 52.) Because Clayton claims she provided her PHI to several medical centers in order to receive healthcare services and the medical centers entrusted her PHI to Blackbaud, it is plausible that Blackbaud's software was used "to make the information available to [Clayton] or a provider of health care at the request of [Clayton] or a provider of health care" or "for the diagnosis, treatment, or management of [Clayton's] medical condition[.]" Cal. Civ. Code § 56.06(b) (West 2021). Accordingly, California Plaintiffs plausibly allege that Blackbaud constitutes a "provider of health care" under Cal. Civ. Code § 56.06(b).

In summary, the court grants in part and denies in part Blackbaud's Motion to Dismiss California Plaintiffs' CMIA claims. (ECF No. 110.) The court grants Blackbaud's Motion to Dismiss as to California Plaintiffs Eisen's, Estes', and Regan's CMIA claims because they do not allege that their "medical information" was compromised in the Ransomware Attack. (*Id.*) However, the court denies Blackbaud's Motion to Dismiss as to California Plaintiff Clayton because she sufficiently asserts that her "medical information" was exposed as a result of the Ransomware Attack and that Blackbaud qualifies as a "medical provider" under the CMIA. (*Id.*)

C. Florida Deceptive and Unfair Trade Practice Act Claims

FDUTPA proscribes "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce . . . ." Fla. Stat. Ann. § 501.204 (West 2021). "To enforce this proscription, the Act has created a private cause of action for damages, Fla. Stat. § 501.211(2), and for declaratory or injunctive relief, Fla. Stat. § 501.211(1)." *Klinger v. Weekly World News, Inc.*, 747 F. Supp. 1477, 1479 (S.D. Fla. 1990). In

the present case, Florida Plaintiffs William Carpenella and Dorothy Kamm (collectively, "Florida Plaintiffs") assert FDUTPA claims for damages as well as declaratory and injunctive relief. (ECF No. 77 at 233 ¶ 929 – 237 ¶ 944.)

To state a claim for damages under FDUTPA, a plaintiff must allege: "(1) a deceptive act or unfair practice; (2) causation; and (3) actual damages." *City First Mortgage Corp. v. Barton*, 988 So. 2d 82, 86 (Fla. Dist. Ct. App. 2008). Here, Florida Plaintiffs allege that Blackbaud committed nine (9) deceptive acts or unfair practices. (ECF No. 77 at 234-35 ¶ 933.) In summary, they claim that Blackbaud:

- Failed to adopt reasonable security measures and adequately notify customers and Plaintiffs of the data breach;
- Misrepresented that certain sensitive PII was not exposed during the breach, it would protect Plaintiffs' PII, and it would adopt reasonable security measures; and
- Concealed that it did not adopt reasonable security measures.

(*Id.*) As a result of such alleged deceptive acts or unfair practices, Florida Plaintiffs assert that they suffered damages such as "fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information." (*Id.* at 236 ¶ 943.)

Viewing the CCAC in the light most favorable to Florida Plaintiffs, Florida Plaintiffs have failed to sufficiently establish the "actual damages" leg of the "FDUTPA liability tripod." *Rollins, Inc. v. Butland*, 951 So. 2d 860, 871 (Fla. Dist. Ct. App. 2006). Under FDUTPA, a plaintiff may recover "economic damages related ***solely*** to a product or service purchased in a consumer transaction infected with unfair or deceptive trade practices or acts." *Delgado v. J.W. Courtesy Pontiac GMC-Truck, Inc.*, 693 So. 2d 602, 606 (Fla. Dist. Ct. App. 1997) (emphasis added). A plaintiff may not recover for "damage to property other than the property that is the subject of the consumer transaction." Fla. Stat. Ann. § 501.212(3) (West 2021). Thus, FDUTPA "entitles a

consumer to recover damages attributable to the diminished value of the goods or services received, but does not authorize recovery of consequential damages to other property attributable to the consumer's use of such goods or services." *Schauer v. Morse Operations, Inc.*, 5 So. 3d 2, 7 (Fla. Dist. Ct. App. 2009).

In the present case, the data management software Blackbaud provided to Social Good Entities is "the property that is the subject of the consumer transaction." Fla. Stat. Ann. § 501.212(3) (West 2021). Throughout the CCAC, Florida Plaintiffs contend that Social Good Entities purchased software solutions from Blackbaud to store, analyze, and manage their patrons' data. (*See, e.g.*, ECF No. 77 at 6 ¶ 12, 13-14 ¶ 30, 112 ¶ 424, 115 ¶ 431.) They do not maintain that Social Good Entities sold or licensed their patrons' data to Blackbaud. Thus, like the subject of a sale of photo editing software is the software and not the pictures that the purchaser edits with the software, the subject of Social Good Entities' purchase of data management software is the software rather than the data they managed with the software. Accordingly, Florida Plaintiffs can only recover for damages to the data management products organizations purchased from Blackbaud to maintain Florida Plaintiffs' PII.

However, Florida Plaintiffs allege no such damages. Fraud and identity theft, time and money spent on mitigation, an increased risk of fraud and identity theft, and loss of value of Florida Plaintiffs' PII do not constitute harm to the data management products Social Good Entities purchased from Blackbaud to maintain Florida Plaintiffs' data. (*Id.* at 236 ¶ 943.) Instead, such injuries constitute harm to Florida Plaintiffs' bank accounts, emotional well-being, and data. As Florida Plaintiffs have not alleged damages to "the property that is the subject of the consumer transaction[,]" they have failed to sufficiently assert "actual damages" under FDUTPA. Fla. Stat.

Ann. § 501.212(3) (West 2021). Therefore, the court grants Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA claims seeking damages. (ECF No. 110.)

Although Florida Plaintiffs fail to state a claim for damages under FDUTPA, they adequately state a claim for injunctive relief under FDUTPA. FDUTPA makes "declaratory and injunctive relief available to a broader class of plaintiffs than could recover damages." *Smith v. Wm. Wrigley Jr. Co.*, 663 F. Supp. 2d 1336, 1339 (S.D. Fla. 2009). Thus, to state a claim for injunctive relief, "the plain language of the statute requires a plaintiff to allege that the defendant engaged in a deceptive act or practice in trade or commerce, § 501.204(1), and that the plaintiff be a person 'aggrieved' by the deceptive act or practice, § 501.211(1)." *Klinger*, 747 F. Supp. at 1480; *see also Wyndham Vacation Resorts, Inc. v. Timeshares Direct, Inc.*, 123 So. 3d 1149, 1152 (Fla. Dist. Ct. App. 2012).

Blackbaud presently does not dispute that Florida Plaintiffs have alleged that Blackbaud engaged in a deceptive act or unfair practice. (*See* ECF No. 110-1.) Florida Plaintiffs have also plausibly pled that they were "aggrieved" by Blackbaud's allegedly deceptive acts or unfair practices. They maintain that Blackbaud's security failures contributed to the Ransomware Attack that compromised their data, exposing them to fraud and identity theft and diminishing the value of their PII. (ECF No. 77 at 234 ¶ 933 – 236 ¶ 943.) Florida Plaintiffs further assert that Blackbaud's misrepresentations and omissions about its security efforts and the scope of the Ransomware Attack prompted them to take mitigation efforts out of fear that they were at an increased risk for fraud or identity theft. (*Id.*) As Florida Plaintiffs have sufficiently alleged a claim for declaratory and injunctive relief under FDUTPA, the court denies Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA declaratory and injunctive relief claims. (ECF No. 110.)

D. New Jersey Consumer Fraud Act Claims

Blackbaud contends that New Jersey Plaintiffs Martin Roth's and Rachel Roth's (collectively, "New Jersey Plaintiffs") claims under the NJCFA should be dismissed for failure to state a claim. (ECF No. 110-1 at 31-35.) Blackbaud asserts its services do not fall within the purview of the NJCFA because it sells services to sophisticated businesses and entities, not the general public. (ECF No. 110-1 at 32.) As such, New Jersey Plaintiffs are not "consumers" of its services protected by the NJCFA. To state a NJCFA claim, a "consumer" must allege sufficient facts to demonstrate (1) unlawful conduct by the defendant that violates the NJCFA; (2) an ascertainable loss by the plaintiff; and (3) a causal relationship between the unlawful conduct and the ascertainable loss. *Gonzalez v. Wilshire Credit Corp.*, 25 A.3d 1103, 1115 (N.J. 2011) (citing *Lee v. Carter-Reed Co.*, L.L.C., 4 A.3d 561, 576 (N.J. 2010)). "It is well-established that NJCFA claims must meet the heightened pleading requirements of Fed. R. Civ. P. 9(b)." *Lieberson v. Johnson & Johnson Consumer Cos., Inc.*, 865 F. Supp. 2d 529, 538 (D.N.J. 2011) (citing *Frederico v. Home Depot*, 507 F.3d 188, 200 (3d Cir. 2007)). Although Blackbaud does not explicitly contend that New Jersey Plaintiffs lack statutory standing, the court construes Blackbaud's assertion that New Jersey Plaintiffs' claims "fall outside the NJCFA's purview" as a challenge to statutory standing. (ECF No. 110-1 at 31-32, 32 n. 2.)

Statutory standing is a "distinct" concept from Article III and prudential standing. *CGM, LLC v. BellSouth Telecomms., Inc.*, 664 F.3d 46, 52 (4th Cir. 2011). Statutory standing "applies only to legislatively-created causes of action" and concerns "whether a statute creating a private right of action authorizes a particular plaintiff to avail herself of that right of action." *Id.* A motion to dismiss for lack of statutory standing is addressed under Rule 12(b)(6) rather than Rule 12(b)(1) because a "dismissal for lack of statutory standing is properly viewed as a dismissal for failure to

state a claim rather than a dismissal for lack of subject matter jurisdiction." *Id.* (citing *Vaughn v. Bay Envtl. Mgmt., Inc.*, 567 F.3d 1021, 1024 (9th Cir. 2009)).

The NJCFA "provides a private cause of action to consumers who are victimized by fraudulent practices in the marketplace," *Gonzalez*, 25 A.3d at 1114, and prohibits a person from using an "unconscionable commercial practice, deception, fraud," or the like "in connection with the sale or advertisement of any merchandise or real estate." N.J. Stat. Ann. § 56:8-2. Merchandise is defined as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." *Id.* § 56:8- 1. The NJCFA "is not intended to cover every transaction that occurs in the marketplace[,]" instead "[i]ts applicability is limited to consumer transactions which are defined both by the status of the parties and the nature of the transaction itself." *Arc Networks, Inc. v. Gold Phone Card Co.*, 756 A.2d 636, 638 (N.J. Super. Ct. Law Div. 2000) (citing *City Check Cashing, Inc. v. National State Bank*, 582 A.2d 809 (N.J. App. Div. 1990)).

Accordingly, only "consumers" and "commercial competitors" have statutory standing to bring claims under the NJCFA. *800-JR Cigar, Inc. v. GoTo.com, Inc.*, 437 F. Supp. 2d 273, 295-96 (D.N.J. 2006) (citing *Conte Bros. Automotive, Inc. v. Quaker State-Slick 50, Inc.*, 992 F. Supp. 709, 716 (D.N.J. 1998)). In order to recover under the NJCFA as a "consumer," "a Plaintiff must be a consumer of the product *vis-à-vis* the defendant." *In re Managed Care Litig.*, 298 F. Supp. 2d 1259, 1303-04 (S.D. Fla. 2003). Although the NJCFA does not define "consumer," New Jersey courts have interpreted the term to mean "one who uses economic goods and so diminishes or destroys their utilities." *U.S. ex rel. Krahling v. Merck & Co., Inc.*, 44 F. Supp. 3d 581, 607 (E.D. Pa. 2014) (citing *City Check Cashing, Inc. v. Nat'l State Bank*, 582 A.2d 809, 811 (N.J. Super. Ct. App. Div. 1990)).

A plaintiff does not qualify as a "consumer" if they do not purchase a product for consumption. *See Standard Fire Ins. Co. v. MTU Detroit Diesel, Inc.*, No. CIV. A. 07-3827 GEB, 2009 WL 2568199, at *5 (D.N.J. Aug. 13, 2009) (finding that an insurance company asserting an NJCFA claim product defect claim was not a "consumer" because it "did not even purchase the yacht at issue"); *In re Schering-Plough Corp. Intron/Temodar Consumer Class Action*, No. 2:06-CV-5774(SRC), 2009 WL 2043604, at *31 (D.N.J. July 10, 2009) ("Products and services that are purchased for consumption or use in the operation of a business are covered by the NJCFA.") (concluding that third-payor payers who did not "use or consume the drugs they purchase[d]" were not "consumers" of the drugs they purchased); *Windsor Card Shops, Inc. v. Hallmark Cards, Inc.*, 957 F. Supp. 562, 567 n.6 (D.N.J. 1997) (holding that a corporation "cannot sue as a consumer of goods under [the] NJCFA" when it "purchased the goods at wholesale to sell to its store customers").

Here, New Jersey Plaintiffs are not "consumers" entitled to the protection of the NJCFA. Martin Roth alleges that Blackbaud maintained his data as a result of his relationship with Joseph Kushner Hebrew Academy and claims that the school retained his data because his "children attended Joseph Kushner Hebrew Academy and he also made charitable donations during the time his children attended the school." (ECF No. 77 at 66 ¶ 231.) Such assertions do not plausibly establish that Martin Roth was a "consumer" of Blackbaud's data management services. They do not suggest that Martin Roth knew that Blackbaud existed or managed his data on behalf of Joseph Kushner Hebrew Academy, let alone that he purchased and used Blackbaud's services. Further, Martin Roth's donation to Joseph Hebrew Academy does not render him a "consumer" of philanthropy. Donors are not "consumers" under the NJCFA because they are "not being approached in their commonly accepted capacity as consumers" and a donation "involves neither

commercial goods nor commercial services." *See Del Tufo v. Nat'l Republican Senatorial Comm.*, 591 A.2d 1040, 1042 (N.J. Super. Ct. Ch. Div. 1991). Thus, the CCAC does not plausibly allege that Martin Roth purchased any services for consumption.

Similarly, Rachel Roth does not plausibly contend that she is a "consumer" of Blackbaud's services. Rachel Roth claims that Blackbaud stored her data as a result of her attendance at Joseph Kushner Hebrew Academy from 2005 through 2014. (ECF No. 77 at 68 ¶¶ 239, 240.) But like Martin Roth, she does not assert that she purchased or used Blackbaud's services, knew Blackbaud existed, or perceived that Blackbaud managed her data. (*See id.* at 67 ¶ 238 – 69 ¶ 246.)

Therefore, New Jersey Plaintiffs fail to state claims under the NJCFA because they do not plausibly allege that they are "consumers" of services entitled to the NJCFA's protection. Accordingly, the court grants Blackbaud's Motion to Dismiss New Jersey Plaintiffs' NJCFA claims. (ECF No. 110.)

E. New York General Business Law § 349 Claims

New York Plaintiffs Ralph Peragine and Karen Zielinski (collectively, "New York Plaintiffs") assert claims under GBL § 349. (ECF No. 77 at 342 ¶ 1443 – 344 ¶ 1451.) To bring a claim for a violation of GBL § 349, a plaintiff must plausibly allege three elements: (1) "the challenged act or practice was consumer-oriented;" (2) the act or practice "was misleading in a material way;" and (3) "the plaintiff suffered injury as a result of the deceptive act[.]" *Stutman v. Chem. Bank*, 731 N.E.2d 608, 611 (N.Y. 2000). Blackbaud contends that New York Plaintiffs have failed to establish the first element of a GBL § 349 claim.

An act or practice is "consumer-oriented" if it has "a broader impact on consumers at large." *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 647 N.E.2d 741, 744 (N.Y. 1995). Thus, "[p]laintiffs must allege conduct that implicates the public interest,

something more than a single-shot consumer transaction or a contract dispute unique to the parties." *Phifer v. Home Savers Consulting Corp.*, No. 06 CV 3841 (JG), 2007 WL 295605, at *5 (E.D.N.Y. Jan. 30, 2007) (citing *Teller v. Bill Hayes, Ltd.*, 630 N.Y.S.2d 769 (N.Y. App. Div. 1995)). However, GBL § 349 does "not impose a requirement that consumer-oriented conduct be directed to all members of the public[.]" *Plavin v. Grp. Health Inc.*, 146 N.E.3d 1164, 1170 (N.Y. 2020). The "consumer-oriented" act or practice requirement has been "construed liberally." *New York v. Feldman*, 210 F. Supp. 2d 294, 301 (S.D.N.Y. 2002).

Contrary to Blackbaud's assertions, New York Plaintiffs adequately plead that Blackbaud's allegedly deceptive acts were "consumer-oriented." New York Plaintiffs allege that Blackbaud engaged in nine (9) deceptive acts or practices in violation of GBL § 349. (ECF No. 77 at 342-43 ¶ 1444.) Essentially, they assert that Blackbaud:

- Failed to implement reasonable security measures and timely and adequately notify Blackbaud customers, New York Plaintiffs, and New York Subclass members of the data breach;
- Misrepresented its security measures and the scope of the data breach; and
- Concealed the fact that it did not reasonably secure the PII and/or PHI of New York Plaintiffs and New York Subclass members.

(*Id.*)

Viewing the CCAC in the light most favorable to New York Plaintiffs, New York Plaintiffs plausibly claim that such deceptive acts had "a broader impact on consumers at large." *Oswego*, 647 N.E.2d at 744. They maintain that Blackbaud's misrepresentations and omissions deceived donors, patients, students, and congregants in New York to believe they did not need to take actions to secure their identities because their data was not exposed. (ECF No. 77 at 6 ¶ 11, 343-44 ¶ 1446.) They also assert that Blackbaud's deceptions misled donors, patients, students, and congregants in New York about the adequacy of Blackbaud's data security. (*Id.* at 6 ¶ 11, 343 ¶ 1445.) Specifically, New York Plaintiffs claim that they would not have entrusted their PII and/or

PHI to a Social Good Entity if they had known that one of the primary cloud computing vendors the entity entrusted with their PII and/or PHI failed to maintain adequate data security. (*Id.* at 69-70 ¶ 248, 72 ¶ 258.) Such allegations suggest that Blackbaud's allegedly deceptive acts caused donors, patients, students, and congregants in New York to suffer avoidable injuries such as identity theft and diminished data value. Accordingly, it is plausible that Blackbaud's misrepresentations and omissions impacted a broad segment of New York consumers.

As privity is not required to state a claim under GBL § 349, it is irrelevant that New York Plaintiffs are not direct consumers of Blackbaud. *See Bildstein v. MasterCard Int'l*, Inc., No. 03 CIV.9826I(WHP), 2005 WL 1324972, at *3 (S.D.N.Y. June 6, 2005).

> While the typical case under section 349 generally involves claims arising directly out of a commercial transaction between a plaintiff consumer and a defendant seller, neither the text of the statute nor the case law establishes this requirement. The phrase "commercial transaction" can be found nowhere in the plain language of the statute, and section 349(h) specifically empowers "[a]ny person who has been injured by reason of any violation of this section" to bring an action. GBL § 349(h). Indeed, "[t]here is no requirement of privity, and victims of indirect injuries are permitted to sue under the Act."

In re Methyl Tertiary Butyl Ether Products Liab. Litig., 175 F. Supp. 2d 593, 630-31 (S.D.N.Y. 2001) (quoting *Vitolo v. Dow*, 634 N.Y.S.2d 362 (N.Y. Sup. Ct. 1995)). "The critical question, then, is whether the matter affects the public interest in New York, not whether the suit is brought by a consumer or a competitor." *Securitron Magnalock Corp. v. Schnabolk*, 65 F.3d 256, 264 (2d Cir. 1995).

Furthermore, Blackbaud's allegedly deceptive acts are similar to other acts that courts have found to be "consumer-oriented" under GBL § 349. Conduct has been held to be sufficiently consumer-oriented to satisfy the statute "where it involved 'an extensive marketing scheme,' where it involved the 'multi-media dissemination of information to the public,' and where it constituted a standard or routine practice that was 'consumer-oriented in the sense that [it]

potentially affect[ed] similarly situated consumers.'" *Tomassini v. FCA U.S. LLC*, No. 3:14-CV-1226 MAD/DEP, 2015 WL 3868343, at *4 (N.D.N.Y. June 23, 2015) (quoting *N. State Autobahn, Inc. v. Progressive Ins. Grp. Co.*, 953 N.Y.S.2d 96, 102 (N.Y. App. Div. 2012)). Additionally, "courts have allowed claims under Section 349 where misleading statements are made to third parties resulting in harm to consumers." *Bose v. Interclick, Inc.*, No. 10 CIV. 9183 DAB, 2011 WL 4343517, at *8 (S.D.N.Y. Aug. 17, 2011) (citing *Securitron*, 65 F.3d at 264; *Kuklachev v. Gelfman*, 600 F. Supp. 2d 437, 476 (E.D.N.Y. 2009)).

In the present case, New York Plaintiffs assert that Blackbaud's public misrepresentations about the scope of the Ransomware Attack misled Plaintiffs into believing they did not need to take mitigation measures against identity theft and fraud. (ECF No. 77 at 343-44 ¶ 1446.) Such conduct is akin to an "extensive marketing scheme" utilizing "multi-media dissemination of information to the public" since Blackbaud allegedly promulgated misrepresentations about the extent of the Ransomware Attack through media interviews, its website, and Social Good Entities. (*Id.* at 9 ¶ 20, 16 ¶ 36, 70 ¶ 251, 72-73 ¶ 261, 138 ¶ 499.) New York Plaintiffs also claim that "misleading statements [were] made to third parties resulting in harm to consumers" because they contend Blackbaud's misrepresentations about its data security to its customers prevented consumers from protecting their data. (*Id.* at 6 ¶ 11, 69-70 ¶ 248, 72 ¶ 258, 343 ¶ 1445.)

Since New York Plaintiffs have sufficiently alleged that Blackbaud engaged in acts in violation of GBL § 349 that were "consumer-oriented," the court denies Blackbaud's Motion to Dismiss New York Plaintiffs' GBL § 349 claims. (ECF No. 110.)

F. Pennsylvania Unfair Trade Practices and Consumer Protection Law Claim

Pennsylvania Plaintiff Christina Duranko ("Pennsylvania Plaintiff") asserts a claim under the UTPCPL. (ECF No. 77 at 362 ¶ 1531 – 365 ¶ 1542.) The UTPCPL provides a private cause

of action to "[a]ny person who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by any person of a method, act or practice declared unlawful" by the Act. 3 Pa. Stat. Ann. § 201-9.2 (West 2021). To maintain a private right of action under the UTPCPL, "a plaintiff must show that he justifiably relied on the defendant's wrongful conduct or representation and that he suffered harm as a result of that reliance." *Yocca v. Pittsburgh Steelers Sports, Inc.*, 854 A.2d 425, 438 (Pa. 2004); *see also Hunt v. U.S. Tobacco Co.*, 538 F.3d 217, 221 (3d Cir. 2008). "It is the plaintiff's burden to prove justifiable reliance in the complaint." *Riviello v. Chase Bank USA, N.A.*, No. 3:19-CV-0510, 2020 WL 1129956, at *4 (M.D. Pa. Mar. 4, 2020) (citing *Weinberg v. Sun Co., Inc.*, 777 A.2d 442, 446 (Pa. 2001)). Pennsylvania Plaintiff has failed to meet this burden.

Pennsylvania Plaintiff's UTPCPL claim is premised on both Blackbaud's alleged misrepresentations and its alleged omissions. She asserts that Blackbaud misrepresented that it would protect the privacy and confidentiality of her information, the scope of the Ransomware Attack, and that it would comply with common law and statutory duties pertaining to the security and privacy of her information. (ECF No. 77 at 362-63 ¶ 1535). She also maintains that Blackbaud omitted that it did not adequately secure her information or comply with common law and statutory duties pertaining to the security and privacy of her information. (*Id.*)

However, Pennsylvania Plaintiff does not sufficiently allege that she relied on such alleged misrepresentations and omissions. She claims that she was "required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services[,]" her PHI "was in turn provided to Blackbaud to be held for safekeeping[,]" and she suffered injuries as a result of her "reliance" on Blackbaud's misrepresentations and omissions. (*Id.* at 85 ¶ 310, 364 ¶ 1541.) But

the CCAC is bereft of allegations suggesting that Pennsylvania Plaintiff knew that Blackbaud maintained her data or was exposed to representations Blackbaud made to her or her healthcare provider. In fact, the CCAC does not even assert that Pennsylvania Plaintiff knew that Blackbaud existed. Pennsylvania Plaintiff does maintain that she "would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security." (*Id.* at 84-85 ¶ 309.) However, such an assertion is nothing more than a conclusory allegation. Thus, even viewing the CCAC in the light most favorable to Pennsylvania Plaintiff, Pennsylvania Plaintiff has failed to adequately establish the reliance requirement of a UTPCPL claim.

Recognizing the weakness of her claim, Pennsylvania Plaintiff asks the court to "hold that [her] UTPCPL theories based on Blackbaud's omissions may nonetheless proceed" because reliance is not an element of an omission-based UTPCPL claim. (ECF Nos. 123 at 38 n.11; 137 at 58:13-17.) Such an interpretation of UTPCPL case law "relaxes the 'justifiable reliance' element of a UTPCPL claim far too much[.]" *In re Rutter's Inc. Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 29054, at *20 (M.D. Pa. Jan. 5, 2021). Pennsylvania courts "have presumed reliance [in UTPCPL cases] only under narrow circumstances not present here, such as securities fraud[] and manufacturing defects[.]" *Moore v. Angie's List, Inc.*, 118 F. Supp. 3d 802, 817 n.8 (E.D. Pa. 2015).

Pennsylvania Plaintiff correctly notes that plaintiffs were not required to establish reliance to prove their omission-based UTPCPL claims in *Drayton v. Pilgrim's Pride Corp.*, No. 03-2334, 2004 WL 765123 (E.D. Pa. Mar. 31, 2004) and *Zwiercan v. Gen. Motors Corp.*, 58 Pa. D. & C. 4th 251 (Pa. Com. Pl. 2002). (ECF No. 123 at 37.) However, *Drayton* and *Zwiercan* stand for the

limited proposition that reliance can be presumed in UTPCPL actions where a manufacturer knows of a dangerous safety defect that customers would be unable to discover themselves. *Drayton*, 2004 WL 765123, at *7 (citing *Zwiercan*, 58 Pa. D. & C. 4th 251). *Drayton* presumed the reliance element of a UTPCPL claim against defendant poultry processing plants by a plaintiff whose husband died from ingestion of listeria-contaminated meat, while *Zwiercan* did not require a plaintiff car purchaser to establish the reliance element in a UTPCPL action against a defendant car manufacturer for dangerously defective front seats. 2004 WL 765123, at *7; 58 Pa. D. & C. 4th 251. In other words, *Drayton* and *Zwiercan* both involved manufacturers of potentially-dangerous products that "allegedly knew their product was adulterated and therefore dangerous, and would therefore have a duty to advise unsophisticated consumers of that material fact." *Drayton*, 2004 WL 765123, at *7 (citing *Zwiercan*, 58 Pa. D. & C. 4th 251). Acknowledging that the decision to presume reliance in both cases was driven by the life-threatening consequences of the omissions at issue, the court in *Drayton* explicitly noted that "in normal UTPCPL false advertising claims reliance is required[.]" *Id.*

The facts of the present case are more similar to a "normal UTPCPL false advertising claim[]" than to the facts in *Drayton* and *Zwiercan*. *Id.* Defendants in data breach cases cannot be "aptly compared to a car manufacturer or a meat-processing plant" because they are "not duty-bound, like a car manufacturer with front seat defects or meat-processer with a listeria outbreak, to alert customers or state or federal officials as to any potential data-security issues." *In re Rutter's*, 2021 WL 29054, at *21. Here, Pennsylvania Plaintiff did not purchase a potentially-dangerous product that would impose a duty on Blackbaud to notify Pennsylvania Plaintiff or government officials of any potential data-security issues. Unlike the omissions in *Drayton* and

Zwiercan, Blackbaud's alleged omissions about its data security practices did not expose its customers and their patrons to life-or-death consequences.

Pennsylvania Plaintiff's UTPCPL data breach claim also differs from the UTPCPL product defect claims at issue in *Drayton* and *Zwiercan* because "the plaintiffs in *Zwiercan* and *Drayton* were totally unable to establish the reliance element—in both cases, 'the unsophisticated Plaintiff is at the mercy of the Defendant to inform her of a known safety defect.'" *Id.* at *21 (quoting *Zwiercan*, 58 Pa. D. & C. 4th 251). In contrast, Blackbaud made representations about its security infrastructure and the scope of the Ransomware Attack in the present case. Pennsylvania Plaintiff does not assert that she relied on such representations when deciding to entrust her data to her healthcare provider and Blackbaud. Given that this case does not involve a potentially-dangerous product and Pennsylvania Plaintiff could have established the reliance element of a UTPCPL claim based on Blackbaud's alleged misrepresentations, the court finds that the reliance presumption enunciated in *Drayton* and *Zwiercan* does not apply here. This conclusion is supported by the United States District Court for the Middle District of Pennsylvania's decision not to extend the reliance presumption articulated in *Drayton* and *Zwiercan* to the data breach context in *In re Rutter's*. 2021 WL 29054, at *21.

As Pennsylvania Plaintiff does not sufficiently assert that she justifiably relied on Blackbaud's alleged misrepresentations and omissions and a presumption of reliance does not apply to the facts of this case, Pennsylvania Plaintiff has failed to establish the justifiable reliance requirement of a UTPCPL claim. Accordingly, the court grants Blackbaud's Motion to Dismiss Pennsylvania Plaintiff's UTPCPL claim. (ECF No. 110.)

G. South Carolina Data Breach Security Act Claims

South Carolina Plaintiffs Latricia Ford and Clifford Scott (collectively, "South Carolina Plaintiffs") advance SCDBA claims under S.C. Code Ann. § 39-l-90(a). (ECF No. 77 at 370 ¶ 1574 – 372 ¶ 1581.) S.C. Code Ann. § 39-l-90(A) requires a person conducting business in South Carolina and "***owning or licensing*** computerized data or other data that includes personal identifying information" to notify South Carolina residents in the event of a data breach. S.C. Code Ann. § 39-1-90(A) (West 2021) (emphasis added). Blackbaud maintains that it is not liable under the SCDBA because it does not "own[] or licens[e]" data. (ECF No. 110-1 at 41-44 (citing S.C. Code Ann. § 39-l-90(A) (West 2021).) The court agrees.

The CCAC features the conclusory assertion that Blackbaud "is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A)." (ECF No. 77 at 371 at ¶ 1575.) However, it does not "contain sufficient factual matter" to plausibly allege that Blackbaud "own[s] or licens[es]" data. *Iqbal*, 556 U.S. at 678; S.C. Code Ann. § 39-l-90(A) (West 2021). The CCAC suggests that Blackbaud possesses data, contending that Social Good Entities "entrusted Plaintiffs' and class members' data to Blackbaud" and Blackbaud "hosted" information from Social Good Entities. (ECF No. 77 at 7-8 ¶ 15, 8 ¶ 16, 11 ¶ 24.) But it does not assert that Blackbaud has an ownership interest or other form of legal entitlement to the data it receives from Social Good Entities and their patrons. Possession may be a necessary condition of "owning or licensing[,]" but it is not sufficient to establish "owning or licensing[.]" S.C. Code Ann. § 39-l-90(A) (West 2021). In fact, South Carolina Plaintiffs' counsel admitted at the hearing that they "alleged the bare minimum in [their] complaint" and professed "it's really difficult to stand here and argue that [Blackbaud is] without a doubt an owner or licensor without additional information." (ECF No. 137 at 60:1-3.) "Labels,

conclusions, recitation of a claim's elements, and naked assertions devoid of further factual enhancement will not suffice to meet the Rule 8 pleading standard." *ACA Fin. Guar. Corp. v. City of Buena Vista, Virginia*, 917 F.3d 206, 211 (4th Cir. 2019). As the CCAC contains nothing more than a naked assertion that Blackbaud "is a business that owns or licenses" data, South Carolina Plaintiffs have failed to plausibly allege that Blackbaud is a business "owning or licensing" data under S.C. Code Ann. § 39-l-90(A). (ECF No. 77 at 371 at ¶ 1575); S.C. Code Ann. § 39-l-90(A) (West 2021).

In their Response, South Carolina Plaintiffs assert that they state a claim under the SCDBA because they fulfill the pleading requirements for a SCDBA claim under S.C. Code Ann. § 39-l-90(B). (ECF No. 123 at 39-41.) This argument is unavailing. Unlike S.C. Code Ann. § 39-l-90(A) which only applies to those "***owning or licensing***" data, S.C. Code Ann. § 39-l-90(B) requires a person doing business in South Carolina and "***maintaining*** computerized data or other data that includes personal identifying information that the person does not own" to notify the owner or licensee of the information after a data breach. S.C. Code Ann. § 39-l-90(A)-(B) (West 2021) (emphasis added). Thus, S.C. Code Ann. § 39-l-90(A) and S.C. Code Ann. § 39-l-90(B) provide for separate claims. *See Morgan v. Haley*, No. 2012-CP-4007331, 2013 WL 8335566, at *2 (S.C. Com. Pl. February 27, 2013) (noting that the plaintiff asserted "two separate claims" under S.C. Code Ann. § 39-l-90(A) and S.C. Code Ann. § 39-l-90(B)). Here, South Carolina Plaintiffs explicitly pursue claims under S.C. Code Ann. § 39-l-90(A) and fail to even reference S.C. Code Ann. § 39-l-90(B) in the CCAC. (ECF No. 77 at 370 ¶ 1574 – 372 ¶ 1581.) Since they fail to provide "a short and plain statement of [a S.C. Code Ann. § 39-l-90(B)] claim showing that [they are] entitled to relief[,] South Carolina Plaintiffs do not assert claims under S.C. Code Ann. § 39-l-90(B) in the CCAC. Fed. R. Civ. P. 8(a)(2).

As South Carolina Plaintiffs only assert a SCDBA claim under S.C. Code Ann. § 39-l-90(A) and do not plausibly allege that Blackbaud is a business "owning or licensing" data, the court grants Blackbaud's Motion to Dismiss South Carolina Plaintiffs' SCDBA claims. (ECF No. 110.)

IV. CONCLUSION

For the foregoing reasons, the court **GRANTS IN PART** and **DENIES IN PART** Blackbaud's Motion to Dismiss. (ECF No. 110.) Specifically, the court:

- Denies Blackbaud's Motion to Dismiss California Plaintiffs' CCPA claims;
- Grants Blackbaud's Motion to Dismiss California Plaintiffs Eisen's, Estes', and Regan's CMIA claims;
- Denies Blackbaud's Motion to Dismiss California Plaintiff Clayton's CMIA claim;
- Grants Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA claims seeking damages;
- Denies Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA declaratory and injunctive relief claims;
- Grants Blackbaud's Motion to Dismiss New Jersey Plaintiffs' NJCFA claims;
- Denies Blackbaud's Motion to Dismiss New York Plaintiffs' GBL § 349 claims;
- Grants Blackbaud's Motion to Dismiss Pennsylvania Plaintiff's UTPCPL claim; and
- Grants Blackbaud's Motion to Dismiss South Carolina Plaintiffs' SCDBA claims.

IT IS SO ORDERED.

United States District Judge

August 12, 2021
Columbia, South Carolina